IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor: Lane Lee, et al.

Application No. 09/940,174

Filing Date: 08/27/2001

For: System and Method For Detecting Unauthorized Copying of Encrypted Data

Examiner: Calvin Hewitt, II

Art Unit: 3621

Confirmation No. 5308

Attorney Docket No.: M-12038 US

APPELLANTS' AMENDED OPENING BRIEF

Real Party In Interest

The real party in interest is DPHI Acquisitions, Inc., the present assignee of US Application No. 09/940,174.

Related Appeals and Interferences

There are no other appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 4 – 23 are cancelled.

Claims 1 – 3 are pending and are at least twice rejected by the non-final Office Action dated December 8, 2006.

The rejection of claims 1 – 3 is appealed.

Status of Amendments

An amendment was filed and entered in the response dated September 20, 2006. An amendment under 37 CFR § 41.33 is concurrently filed with this appeal brief to cancel claims 15, 17, 18, 21, and 22. No other amendments have been filed subsequent to the final Office Action dated April 20, 2006.

Summary of Claimed Subject Matter

The claimed subject matter is directed to the detection of unauthorized copies of encrypted data. This detection method may be better understood with regard to the novel optical disks developed by the assignee that contain both a writeable area and a read-only area. The read-only area is mastered during disk manufacture and functions as would a conventional DVD or CD-ROM media. The writeable area has a spiral groove as is used on writeable disks such as DVD-R disks. Such disks were the first practical read-only and writeable combination (ROM/RAM) disks because prior art combination disks were cumbersome affairs to manufacture, requiring numerous masking steps. In contrast, the assignee's ROM/RAM combination disks used a continuous information layer to form both the ROM and RAM features – further details regarding this disk may be located in, for example, in commonly-assigned U.S. Pat. No. 6,580,683.

Consider the content distribution schemes enabled by such a disk – a manufacturer may stamp the ROM area with encrypted content and freely distribute the resulting combination ROM/RAM disks to consumers without requiring payment. The consumer may then gain access to the encrypted content by receiving and writing a key to the writeable area. This present specification discusses such an unlocking of content through use of this combination ROM/RAM disk. However, all content distribution schemes must guard against unauthorized access – thus, the Applicants invented the digital rights management techniques disclosed in the present application. Part of these DRM techniques had to do with the media identifiers discussed by the Applicants, for example, on page 58, line 2 through page 59, line 22. As discussed on page 58, lines 5-7, a first type of media identifier is formed in the ROM area of the disk as it is being mastered with content during manufacture. A second type of identifier is associated with content written into the writeable area (page 58, lines 7-11).

Now consider if a hacker copies an unlocked ROM/RAM disk having a key written to the writeable area – the unlocked ROM portion (having its ROM

identifier) will be written to a writeable area on the bootleg disk. As discussed on page 60, lines 11-20, a disk drive may then read the bootleg disk and determine that it is reading a ROM identifier from the RAM portion. From merely reading the ROM identifier from the RAM portion, the disk drive may then deny functionality to the bootleg disk.

Claim 1 reflects these advantageous features. In particular, the acts of "reading an identifier on the optical disk" and "determining whether the identifier was located in the read-only or the writeable portion of the optical disk" is supported, for example, by page 60, lines 7-13. Similarly, the act of "determining whether the identifier identifies itself as a pre-recorded identifier or as a written identifier" is also supported by page 60, lines 9-15. Finally, the act of "if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk; detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion" is supported by page 60, lines 13-20.

Grounds of Rejection to Be Reviewed on Appeal

1) Whether a conditional limitation in claim 1 may be given no weight by the examiner.

2) Whether U.S. Patent No. 6,782,190 to Morito teaches or suggests the subject matter of Applicants' Claim 1.

3) Whether, under 35 U.S.C. § 103(a), claims 1--3 are unpatentable over U.S. Patent No. 6,782,190 to Morito in view of U.S. Patent No. 6,519,700 to Ram et al.

Argument

1) A conditional claim limitation in claim 1 has been given no weight.

Applicants respectfully note that there is no statutory bar to the use of

conditional limitations in claims. Indeed, Applicants observe that conditional limitations are commonplace in issued U.S. claims – for example, claim 3 of the cited Morito patent uses the conditional limitation of "if the verification information for the medium identifier indicates that the medium is a copy of an original." A perusal of the USPTO database will reveal thousands and thousands of U.S. patents that contain conditional limitations prefaced with "if." In that regard, consider a typical flowchart for a method – most methods will have some sort of conditional node where if condition A exists, the method proceeds with a first course of action and where if condition B exists, the method proceeds with a second course of action. It would be rather curious indeed that U.S. patent law would embrace the patentability of methods but then reject the vast subset of methods that contain conditional acts. However, as set forth in section two of the non-final December 8, 2006 action, a conditional limitation of claim 1 has been given no weight because "language that suggest [sic] or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation." (citing MPEP § 2106 (II)(C)). But a conditional limitation is not an optional step: consider the limitation that was disregarded in the December 6, 2006 action:

> if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk; detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion

This detection is mandatory: if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk, the act of "detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion" must follow – there is no option of not performing this detection whatsoever. In that regard, claim 1 does not say "observing a pre-recorded identifier in the writeable portion and *perhaps* detecting some unauthorized action." There is no optional limitation such as perhaps, maybe, etc. in claim 1. Applicants readily agree that a conditional limitation is being recited – but the claim require acts that determine whether the

"if" limitation is satisfied: it is not an option to determine whether a pre-recorded identifier is being detected in the writeable portion because the claim requires that determination. And if that determination is positive, the detection of an unauthorized action follows. Thus, Applicants respectfully submit that it was clear legal error to give no weight to the conditional limitation of "if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk; detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion."

2) Morito does not teach or suggest the subject matter of claim 1

As discussed in his abstract, Morito is directed to a copy protection scheme for DVD-RAM recorders. In general, the DVD standard as originally developed did not allow consumers to write to DVD disks. Indeed, DVD disks were originally strictly ROM disks that had mastered content impressed onto them during manufacture. In line with such a general theme, Morito is directed to an adaptation of the DVD standard such that only specialized recorders (module 11 of Figure 3) write to writeable DVD disks. These writeable disks have a ROM portion (element 2 of Figure 3) that contains a media identifier written as a bar code. The remaining portion of the disk forms a writeable area (element 3). As discussed in Col. 5, lines 18-28 with regard to Morito's Figure 4, content from database 12 of Figure 3 is written to this writeable area along with a copy of the disk identifier (which Morito denotes as S_d). It may thus be seen that an authorized Morito disk has the identifier S_d in both the ROM and RAM areas. A Morito disk reader checks that it is reading an authorized disk by performing the method of Figure 7. In this method, the reader reads the S_d identifier from the ROM portion and another identifier it obtains from the writeable area – in general, this other identifier will always be S_d but because of the possibility of unauthorized copies Morito refers to it generically as S_p. If S_p does not equal S_d, the Morito reader thus detects it is reading an unauthorized copy (steps s14 and s16 of Figure 7).

It may thus be seen how different Applicants method is – Applicants were

guarding against the copying of ROM data into a RAM portion of another ROM/RAM disk. In that regard, Applicants developed different types of identifiers for their ROM and RAM disk portions. Thus, by having these different types of identifiers, the mere presence of a ROM identifier in the RAM portion identifies a disk as a bootleg. In contrast, Morito must read both the identifier in his ROM portion and the identifier in his RAM portion and compare them to determine if he has a forgery. Indeed, there is no "pre-recorded content" in a Morito disk as would be understood by anyone of ordinary skill in the art – pre-recorded content is what the consumer wants in obtaining such a disk. It is substantive data whereas the identifier in Morita's pre-recorded area is meta-data, not the pre-recorded content the consumer is interested in. Thus, whether a Morita identifier is located in the writeable portion gives a Morito disk drive no cause to detect an unauthorized action. Only by further comparing the Morito identifier (S_p) to the S_d identifier can Morito detect an unauthorized copy. Accordingly, there is no teaching or suggestion in Morito for the act of "determining whether the identifier identifies itself as a pre-recorded identifier or a written identifier" because Morito has only one type of identifier that is stamped into the ROM area during manufacture and then copied and written to the RAM area during a write operation. In addition, Morito has not teaching or suggestion for the act of "if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk; detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion" such that claim 1 and its dependent claims 2 and 3 are patentable over Morito.

3) Claims 1-3 are allowable over the combination of the Morito and Ram References

The Ram reference does nothing to cure the infirmities of the Morito reference discussed above. Accordingly, claims 1, 2, and 3 are patentable over the combination of the Morito and Ram references.

Conclusion

Therefore, in light of the foregoing arguments, Applicants respectfully request the Honorable Board of Appeals to reverse the decision of the Examiner with respect to claims 1 –3.

Respectfully submitted,

Date: March 12, 2008 By: _____

Jonathan W. Hallman
Reg. No. 42,622

Claims Appendix

1. A method of detecting unauthorized actions with respect to content on an optical disk, the optical disk including a read-only portion for pre-recorded content and a writeable portion for written content, the method comprising:

reading an identifier on the optical disk;

determining whether the identifier was located in the read-only or the writeable portion of the optical disk;

determining whether the identifier identifies itself as a pre-recorded identifier or as a written identifier;

and if the identifier identifies itself as a pre-recorded identifier and is located in the writeable portion of the optical disk, detecting an unauthorized action solely from the pre-recorded identifier being located in the writeable portion.

2. The method of claim 1 wherein the reading of the identifier on the optical disk is during a optical disk access operation including one or more of record, play, get play key, copy, open, close and create.

3. The method of claim 2 wherein functionality for the optical disk access operation is revoked after detecting the unauthorized action.

Evidence Appendix

No evidence was submitted under Rules 130, 131, or 132.

Related Proceedings Appendix

There are no related proceedings.